GDPR. Bilancujeme, panika už skončila

JE TO PŘESNĚ ROK OD ZAČÁTKU PLATNOSTI NAŘÍZENÍ ZNÁMÉHO POD ZKRATKOU GDPR. PŘES PŮVODNÍ PONĚKUD KATASTROFICKÉ VIZE SE NIC DĚSIVÉHO NEPŘIHODILO.

Když se před nějakou dobou začalo poprvé mluvit o úpravě povinností souvisejících se správou osobních údajů, vycítila řada firem svou příležitost. Trochu to lze přirovnat k šílenství kolem takzvané chyby Y2K téměř před dvaceti lety. Obrovská mediální kampaň původní, v podstatě správnou myšlenku úpravy a zčásti zpřísnění pravidel zpracování osobních údajů v očích laické veřejnosti vykreslila jako byrokratický, až šikanózní nesmysl, který nám všem jen otravuje život a který si na nás vymysleli úředníci z Bruselu.

Základ velmi negativního vnímání nařízení GDPR spočívá v tom, že laická veřejnost prakticky neví, co všechno osobní údaj může být, jak jej lze využít a jak obrovskou může mít hodnotu. A tak lidé nemají potřebu své osobní údaje chránit. Ochotně je vymění třeba za stažení aplikace pro grafickou úpravu fotografií. Nemají problém s tím, že aplikace pro takovou úpravu například potřebuje přístup k datům uživatele mobilního telefonu a odešle je ke zpracování daleko za hranice Evropské unie.

Mýty spojené s GDPR

Dalším důvodem negativního vnímání nařízení GDPR byla smršť dezinformací, které jsme byli ještě před rokem každodenně vystaveni a která posunula zkratku GDPR mezi výrazy, jež jste už znova nechtěli slyšet, natož dostat v práci úkol s GDPR spojený. Dodnes se s mnoha mýty a jejich vyvracením potýkáme. V profesním, ale i v běžném životě se setkáváme s mnoha špatnými, až úsměvnými implementacemi pravidel GDPR do praxe. Obdivuhodně kreativní byla oblast školství. Tak například jedna mateřská škola zrušila podepsané bačkůrky, jiná ručníky. Další nutila rodiče, aby nesdělovali učitelce, že si jdou pro Janičku Novákovou, ale identifikovali svou dceru pomocí značky, kterou holčička ve školce používá místo podpisu. Takže jste si šli vyzvednout třeba „modrého slona“. A důvod? Někdo by mohl neoprávněně slyšet jméno dítěte. Jinde se zase paní učitelka ptala, zda smí studentovi sdělit po vyzkoušení před celou třídou jeho známku.

Sdružení vlastníků jednotek jsou také vděčné zdroje úsměvných historek. Jedno z nich mělo názor, že se ho GDPR netýká, neboť GDPR je dle jeho názoru aplikovatelné jen na zpracování rodných čísel a tyto údaje oni nemají. Právníci zabývající se touto problematikou tak museli – a dodnes musí – odpovídat i na otázku, zda lékař nebo zdravotní sestra může zavolat pacienta v čekárně jménem. Tato otázka se v praxi zjevně stala tak častá, že se k ní dokonce na svých stránkách vyjádřil Úřad pro ochranu osobních údajů. A zapomenout nelze ani na segment velkých korporací. Tak třeba oblíbená odpověď na otázku, zda a jak se vypořádali s požadavky GDPR, bývá: „To máme vyřešené, to za nás vyřeší/vyřešila naše zahraniční mateřská společnost.“ A poté mi předají graficky velmi hezky vyvedený letáček, ve kterém stojí ujištění, že veškeré zpracování osobních údajů se děje v souladu s pravidly GDPR.

Pokuty jako strašák

Ještě nedávno jsme byli ze všech stran doslova bombardováni hrozbami obrovských pokut, které za porušení pravidel GDPR hrozí. A jaká je realita více než rok po účinnosti GDPR? V České republice se žádné obrovské pokuty zatím nekonají. Diskutovaným byl příklad provozovatele známého internetového obchodu potrestaného pokutou 1,5 milionu korun za nedostatečné zabezpečení osobních údajů nejméně 735 tisíc zákazníků. Zde nutno podotknout, že incident se stal před účinností GDPR.

Úřad pro ochranu osobních údajů na svých webových stránkách zveřejnil jak statistiku udělených pokut, tak v anonymizované verzi dokonce i samotná pravomocná rozhodnutí, kde byla pokuta udělena. V zahraničí už se ale několik odstrašujících případů vyskytlo. Za všechny můžeme jmenovat pokutu 460 000 nizozemské nemocnici za nedostatečně zabezpečené záznamy pacientů. Objevily se zprávy z Velké Británie o úmyslu potrestat sítě hotelů pokutou 99 milionů liber za incident, který se stal v listopadu 2018. Velmi medializované byly i velké pokuty spojené se sociálními sítěmi.

Časté chyby v praxi

Mnoho chyb se v praxi opakuje. Stále dokola a neúnavně je třeba vysvětlovat, že právo zpracovávat osobní údaje se automaticky nerovná nutnosti získat od subjektu údajů souhlas. Kdy a za jakých podmínek je možné založit zpracování osobních údajů na základě souhlasu uděleného subjektem údajů, dělá mnohým správcům problémy pochopit. Měla jsem pocit zmaru, když mi v květnu 2018 zahltilo e-mailovou schránku množství e-mailů, v nichž mě různé společnosti žádaly o udělení souhlasu se zpracováním osobních údajů, kdy mnohé z nich by bylo možné používat jako ukázkové příklady „JAK NE“.

Požadavek jednoduché a srozumitelné řeči dělá mnohým v praxi velké potíže. V situacích, kdy jste v pozici subjektu údajů, seznamujete se s předloženým dokumentem, ale musíte si jej přečíst několikrát, abyste porozuměli jeho obsahu, se sami sebe ptáte: „Kde se stala chyba?“ Nutno podotknout, že tady původní líbivá myšlenka tvůrců GDPR používat jen jednoduchou řeč, doprovázet ji ikonami nebo jinými obrázky, a tak usnadnit orientaci a pochopení textu, se zcela minula účinkem. Zejména při tvorbě informace pro subjekty údajů má autor textu spoustu starostí s tím, aby subjekt údajů (tj. fyzickou osobu, které se údaje týkají) správně poučil a všechny předepsané informace, ke kterým je povinován (některá poučení zopakuje pro jistotu třeba i několikrát), předal. A tak vznikají dlouhé samoúčelné texty, které nikdo nečte. A pokud čte, tak s vypětím všech sil. A další chyby napříč všemi obory? Znovu a znovu i po účinnosti GDPR vídám v pracovních smlouvách nebo ve vstupních dotaznících nesmyslný povinný souhlas zaměstnance se zpracováním jeho osobních údajů, zejména rodného čísla, pro účely realizace pracovněprávního vztahu.

V souladu s GDPR snadno a rychle

Každodenní praxe se v posledním roce musela poprat i v českých poměrech s novou funkcí – pověřencem pro ochranu osobních údajů, také hojně označovaného zkratkou DPO. Správci a zpracovatelé byli dle GDPR povinni pověřence jmenovat. Pověřenec mohl a stále ještě může být jak zaměstnancem správce/zpracovatel, tak i externistou. Nedostatek těchto lidí na pracovním trhu se nechal předpokládat, což otevřelo prostor i pro méně solidní poskytovatele služeb pověřence, které tyto služby neúměrně předražili. Věřím, že časem se trh v tomto ohledu vytříbí a poskytování služeb externího DPO se dostane do standardních kolejí získá zpět reputaci prospěšné služby.

Pokud si ve vaší společnosti stále ještě nejsou jisti, zda zpracování osobních údajů, které provádíte, vykonáváte v souladu s pravidly GDPR, nebo dokonce patříte k těm, kteří s implementací pravidel GDPR stále ještě nezačali, pak bych chtěla doporučit, abyste se nespoléhali na instantní řešení typu „koupím si balíček dokumentů, napíšu do nich název naší společnosti a mám vše vyřešeno“. Takové řešení jde proti smyslu nařízení GDPR, a jestliže by bylo jediným opatřením, které v této souvislosti přijmete, pak by bylo nepochybně i opatřením nedostatečným.

Pokud situaci zjednodušíme na maximum, správce musí být schopen odpovědět „SPLNĚNO“ na všech pět níže uvedených bodů. Pokud si u kteréhokoliv bodu nejste jisti, zcela jistě byste měli problematiku zpracování osobních údajů ve vaší společnosti (znovu) otevřít.

Checklist pro správce zjednodušeně v pěti bodech

Správce musí:

- mít přehled o veškerém zpracování osobních údajů, které provádí;
- mít jasno, na základě jakého právního titulu, pro jaký účel, po jakou dobu údaje zpracovává a komu je zpřístupňuje;
- plnit informační povinnost vůči subjektům údajů;
- vést záznamy o činnostech zpracování;
- přijmout dostatečná technická a organizační opatření k zabezpečení osobních údajů.

PŘÍSTUP TYPU "KOUPÍM SI BALÍČEK DOKUMENTŮ A MÁM GDPR VYŘEŠENO" JDE ZCELA PROTI SMYSLU TOHOTO NAŘÍZENÍ.

Lucie Kalašová
advokátka spolupracující s bpv Braun Partners, s. r. o.